1 CAD data exchange via HyperKVS 2

1.1 Software requirements 2
1.1.1 Internet browser 2
1.1.2 MONA Applet 2
1.1.3 Viewer 2
1.2 Installation and configuration 2
1.2.3 Configuration of routing 3
1.2.4 Configuration of firewall 3
1.3 Import of Volkswagen certificates 4
1.3.1 Settings Mozilla Firefox 4
1.3.2 settings Microsoft Internet Explorer 6

2 CAD data exchange via OFTP2 9

2.1 OFTP installation of a company 9
2.2 OFTP server at Volkswagen 9
2.3 Configuration of firewall 9
2.4 Default settings / ENGDAT parameter 9
2.5 Handover to operation support / connection test 10

3 CONNECT 10

3.1 System requirements 10
3.1.1 Hardware 10
3.1.2 Software 10
3.1.3 Infrastructure and System Environment 11

4 Volkswagen DMS 11

4.1 System requirements 11
4.2 Settings 11

1 CAD data exchange via HyperKVS

1.1 Software requirements

1.1.1 Internet browser

Partner companies have to use a standard internet browser to work with HyperKVS, e.g. Mozilla Firefox or Microsoft Internet Explorer. The used browser need to support encryption via https with a key length of not less than 128 Bit, otherwise access to the HyperKVS is not possible. With access via browser all functions of the KVS system are usable.

1.1.2 MONA Applet

For saving (upload) and downloading documents (CAD-models, describing documents, drawings, etc.) into the persistent file area of HyperKVS and into the temporary file area you need the tool MONA Applet.
With the new MONA Applet the functions import, export, upload, and download can now be introduced into the HyperKVS with usage of new technologies (signed applet). MONA Applet will be run automatically at first use.

Supported browser and java versions:

operation system Windows:
Microsoft Internet Explorer 9 in 32 bit
Mozilla Firefox ESR 17 in 32 bit
Oracle (Sun) Java 1.6.xx or higher in 32 bit

Operation system Linux & Mac:
Mozilla Firefox ESR 17 in 32 bit
Oracle (Sun) Java 1.6.xx or higher in 32 bit

In case of other versions and browsers there might be problems while using, because they are not released for using MONA Applet.

1.1.3 Viewer

HyperKVS offers the possibility of viewing drawings on the directly screen for the users. In this case, the drawing is implicitly converted into TIFF format. Normally the viewer supplied as standard with Windows under ”Imaging for Windows” is adequate for this purpose.

In case of problems regarding visualization due to the file size, we recommend to install the software ”ZGView” for Windows (local administration rights are required). The relevant company is responsible for the program installation.

The TIFF viewer ”CADview” is recommended for UNIX users.

1.2 Installation and configuration

For changing the configuration on company HyperKVS servers, network skills are necessary.
Please pay attention to the following items, explained in details below:

1. HyperKVS dialogue servers that should be used
2. name resolution
3. routing
4. firewall configuration

1.2.1 HyperKVS dialogue server

The following HyperKVS servers are available for companies using KVS of Volkswagen and Audi:

Volkswagen	**Audi**
https://kvs.pfn.vwg:8081	https://kvs.ras.audi.vwg:8081

1.2.2 Name resolution of HyperKVS dialog server

To work with HyperKVS dialogue servers, the server names need to be resolved in an IP address. There are 2 possibilities:

1. DNS name resolution. You can find the following DNS servers on the partner network of Volkswagen:

Volkswagen	**Audi**
193.23.100.200	143.164.6.220

   To assure that the DNS application won't be transmitted to the internet DNS, in certain circumstances a "conditional forwarder" for the domain suffix *.pfn.vwg and/or *.audi.vwg needs to be setup.

2. Local name resolution. Therefore you have to edit the host file of the affected PCs or workstations. Following settings need to be done:

Volkswagen		**Audi**	
kvs.pfn.vwg	193.23.101.225	kvs.ras.audi.vwg	143.164.6.110

   You can find the host files in the directories mentioned below:

Windows NT, 2000, XP	<WINDIR>\system32\drivers\etc\hosts
Unix systems	/etc/hosts

1.2.3 Configuration of routing

For working with HyperKVS dialog servers from your PC or workstation, you have to assimilate the routing under some circumstances. If the routing to the HyperKVS is not assured by a still configured default gateway, there must be an adequate routing entry for every HyperKVS server.
Please find below an example for the configuration of a Windows NT, 2000 or XP PC:

1. push [START] → [execute…] → "cmd"
2. enter the command: route –p add <IP-address of the HyperKVS dialog server> <IP-address of the gateway>

On Unix systems the configuration will be done analog with help of the route command or with a service program like for example smitty on AIX.

1.2.4 Configuration of firewall

The following ports are used by HyperKVS, if necessary they need to be enabled on the firewall:

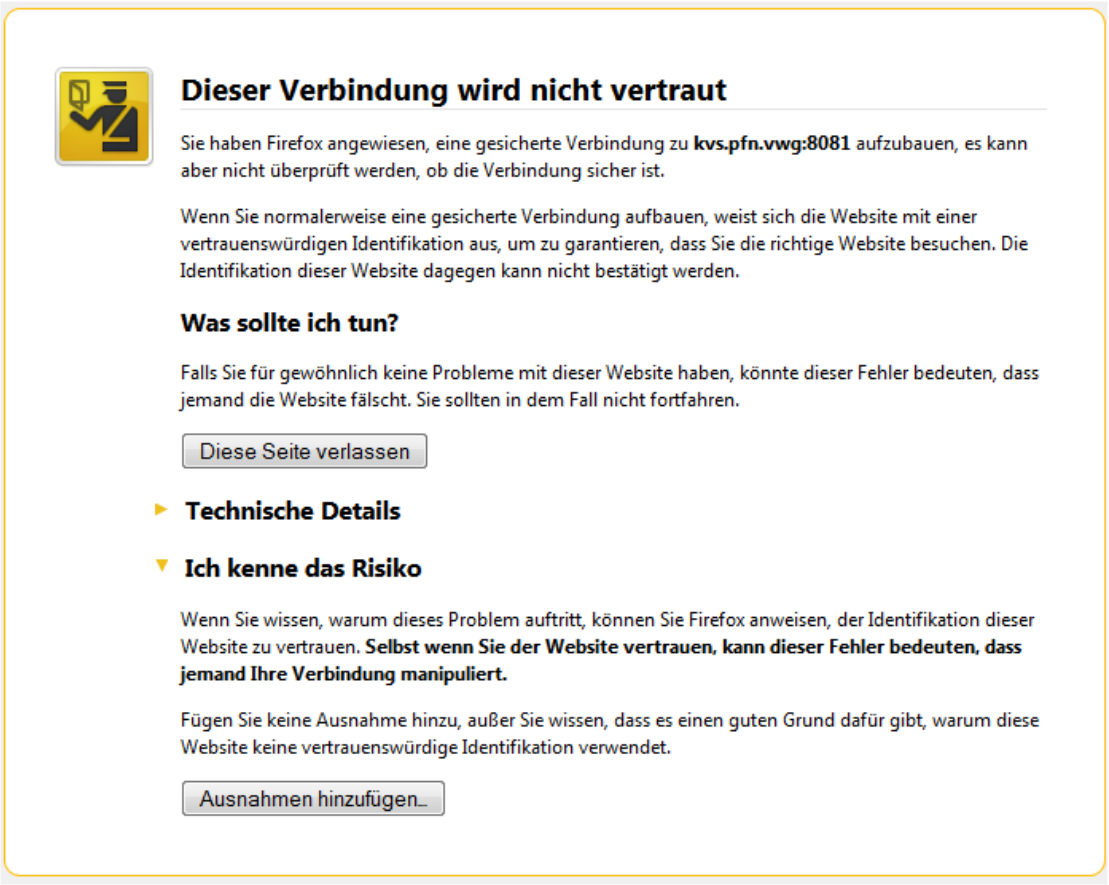
1. HyperKVS with browser
   https – port 8081

1.3 Import of Volkswagen certificates

For the secure link connection via https it is necessary to install certificates of Volkswagen AG to verify the identification of the KVS webpage.
Please find below the information for this procedure regarding web browser Mozilla Firefox and Microsoft Internet Explorer.

1.3.1 Settings Mozilla Firefox

While starting the KVS web page https://kvs.pfn.vwg:8081 (resp. https://kvs.ras.audi.vwg:8081 valid as from 1st of July 2015) without certificate, you will receive the following warning of Firefox:


Dieser Verbindung wird nicht vertraut
Sie haben Firefox angewiesen, eine gesicherte Verbindung zu kvs.pfn.vwg:8081 aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.
Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.
Was sollte ich tun?
Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.
Diese Seite verlassen
Technische Details
Ich kenne das Risiko
Wenn Sie wissen, warum dieses Problem auftritt, können Sie Firefox anweisen, der Identifikation dieser Website zu vertrauen. Selbst wenn Sie der Website vertrauen, kann dieser Fehler bedeuten, dass jemand Ihre Verbindung manipuliert.
Fügen Sie keine Ausnahme hinzu, außer Sie wissen, dass es einen guten Grund dafür gibt, warum diese Website keine vertrauenswürdige Identifikation verwendet.
Ausnahmen hinzufügen...

To clear this warning:

Please download the following certificates under this address:
http://certdist.volkswagen.de/pdcert/certdist/DownloadCA

VW-CA-PROC-06 (file name: VW-CA-PROC-06.cer) and
VW-CA-ROOT-04 (file name: VW-CA-ROOT-04.cer)

Subsequently please import both certificates one after the other as follows:
Firefox menu settings → advanced → certificate → show certificate → choose „certification center" → import → import certificate

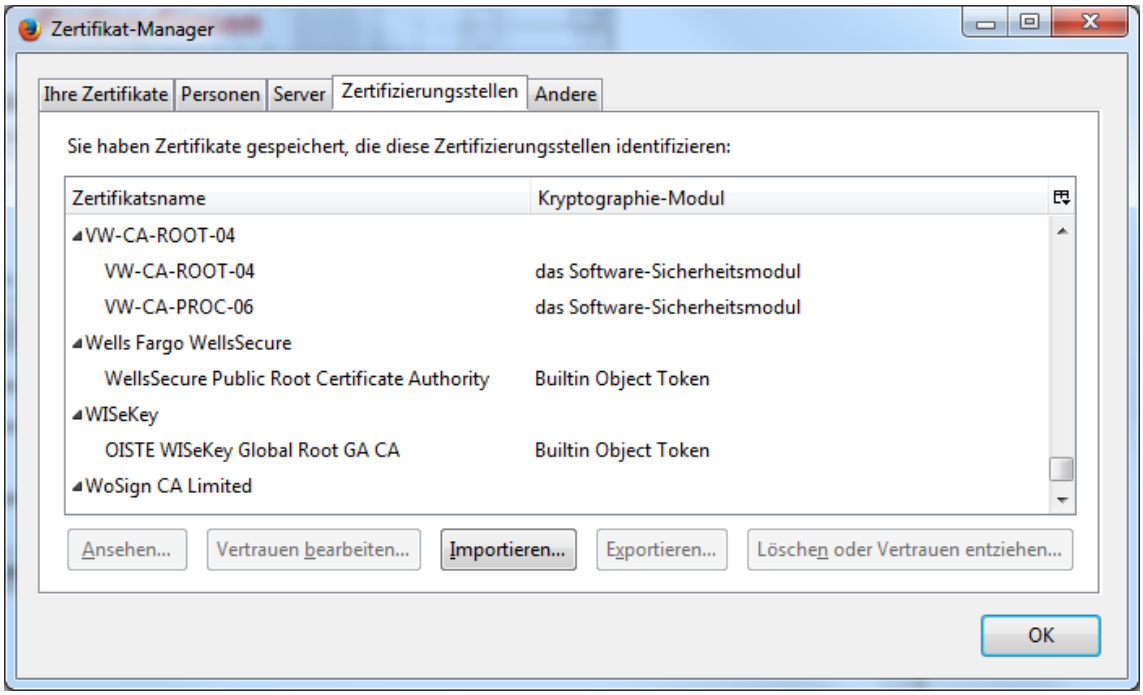
Please confirm the message „Dieser CA vertrauen, um Websites zu identifizieren." that means „trust this CA (certfication authority) to identify web pages" with „OK".

Within the following window / view the choice "Dieser CA vertrauen, um Websites zu identifizieren." must be ticked. ("trust this CA - certfication authority-, to indentify web pages.")

Herunterladen des Zertifikats
Sie wurden gebeten, einer neuen Zertifizierungsstelle (CA) zu vertrauen.
Soll "VW-CA-PROC-06" für die folgenden Zwecke vertraut werden?
Dieser CA vertrauen, um Websites zu identifizieren.
Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.
Dieser CA vertrauen, um Software-Entwickler zu identifizieren.
Bevor Sie dieser CA für jeglichen Zweck vertrauen, sollten Sie das Zertifikat sowie seine Richtlinien und Prozeduren (wenn vorhanden) überprüfen.
Ansicht
CA-Zertifikat überprüfen
OK
Abbrechen

Confirm your choice with „OK".

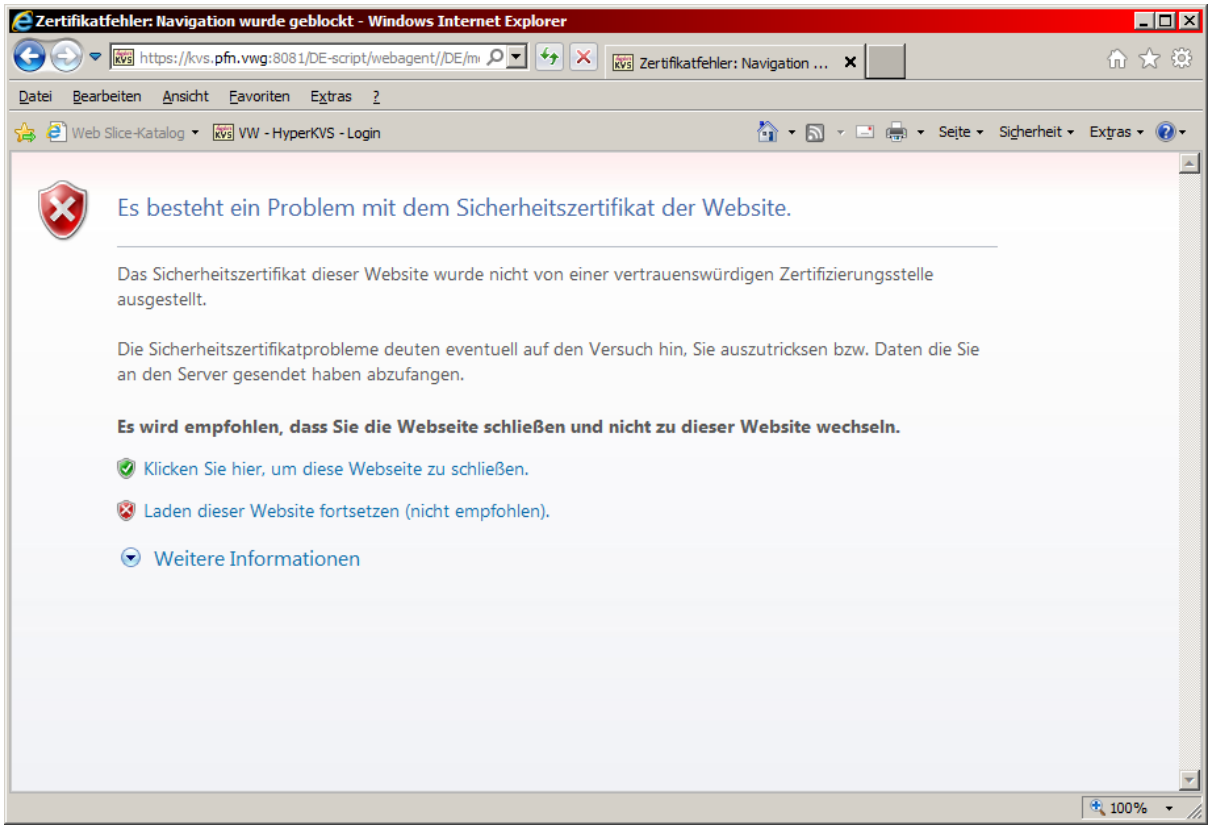
The correct import of the certificate you can check within the menu "certificate manager" of Firefox under menu "certification authorities":



If you see the certificates „VW-CA-PROC-06" as well as „VW-CA-ROOT-04" within the menu "certificate" as shown above, the certificates were successfully installed.

1.3.2 settings Microsoft Internet Explorer

While starting the KVS web page https://kvs.pfn.vwg:8081 (resp. https://kvs.ras.audi.vwg:8081 valid as from 1st July 2015) without certificate, you will receive the following warning within the Internet Explorer:


Zertifikatfehler: Navigation wurde geblockt - Windows Internet Explorer
https://kvs.pfn.vwg:8081/DE-script/webagent//DE/m
Zertifikatfehler: Navigation ...
Datei Bearbeiten Ansicht Favoriten Extras ?
Web Slice-Katalog
VW - HyperKVS - Login
Seite Sicherheit Extras
Es besteht ein Problem mit dem Sicherheitszertifikat der Website.
Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.
Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.
Klicken Sie hier, um diese Webseite zu schließen.
Laden dieser Website fortsetzen (nicht empfohlen).
Weitere Informationen
100%

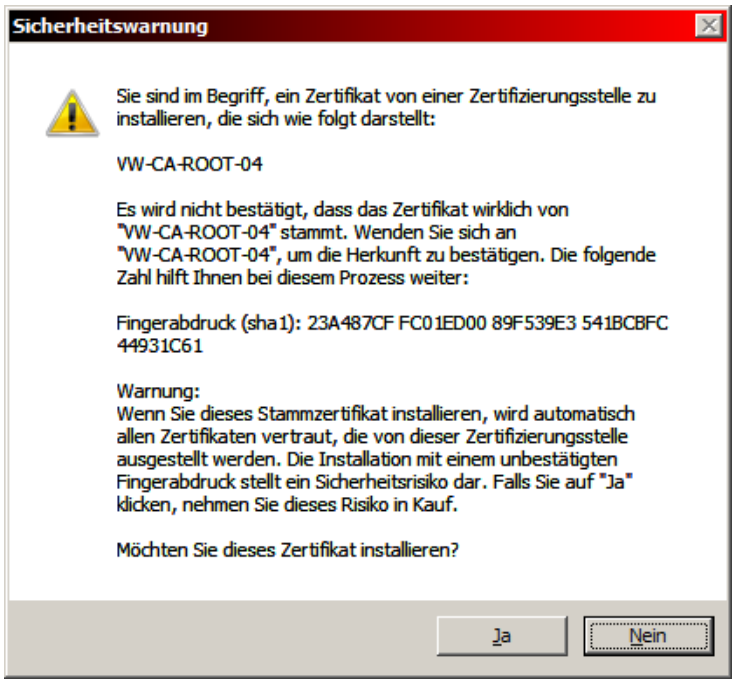
To clear this warning:
Please download the following certificates under this address:
http://certdist.volkswagen.de/pdcert/certdist/DownloadCA

VW-CA-ROOT-04 (data file: VW-CA-ROOT-04.cer) and
VW-CA-PROC-06 (data file: VW-CA-PROC-06.cer)

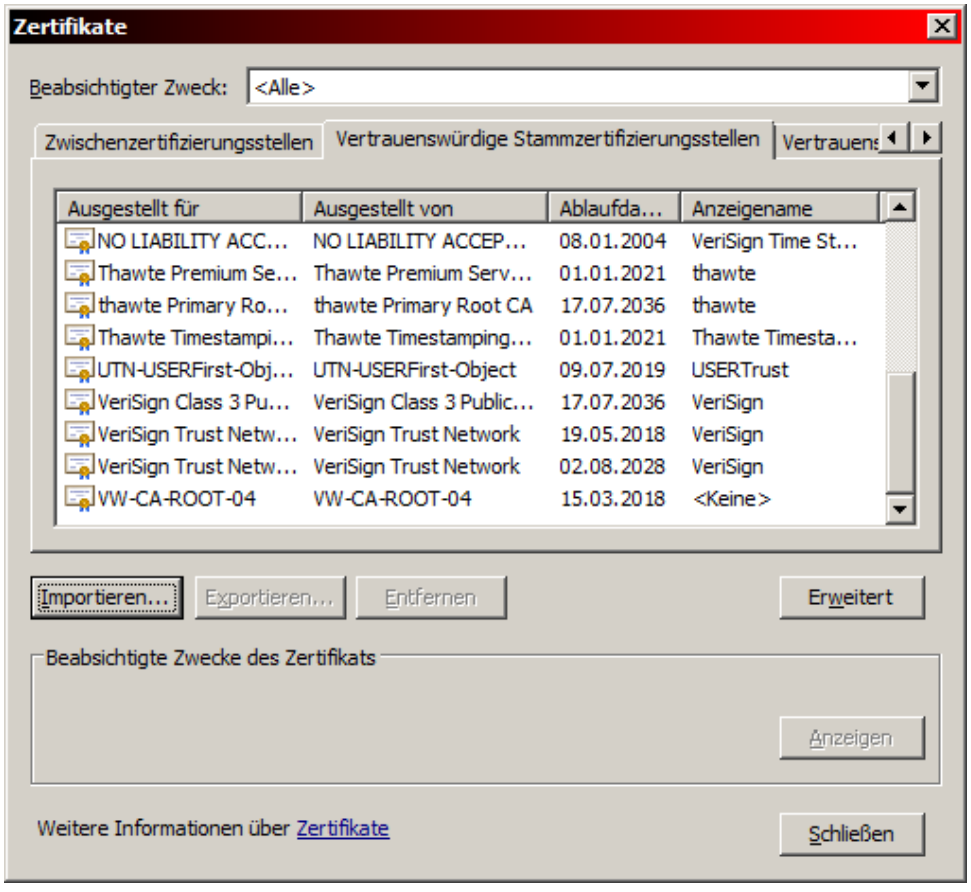
Subsequently please import both certificates one after the other as follows:

VW-CA-ROOT-04:
Internet Explorer under settings/options → content → certificate → choose „trusted **root certification authorities**" → import → import VW-CA-ROOT-04 certificate.

Please confirm the following warning with „Yes".


Sicherheitswarnung
Sie sind im Begriff, ein Zertifikat von einer Zertifizierungsstelle zu installieren, die sich wie folgt darstellt:
VW-CA-ROOT-04
Es wird nicht bestätigt, dass das Zertifikat wirklich von "VW-CA-ROOT-04" stammt. Wenden Sie sich an "VW-CA-ROOT-04", um die Herkunft zu bestätigen. Die folgende Zahl hilft Ihnen bei diesem Prozess weiter:
Fingerabdruck (sha1): 23A487CF FC01ED00 89F539E3 541BCBFC 44931C61
Warnung:
Wenn Sie dieses Stammzertifikat installieren, wird automatisch allen Zertifikaten vertraut, die von dieser Zertifizierungsstelle ausgestellt werden. Die Installation mit einem unbestätigten Fingerabdruck stellt ein Sicherheitsrisiko dar. Falls Sie auf "Ja" klicken, nehmen Sie dieses Risiko in Kauf.
Möchten Sie dieses Zertifikat installieren?
Ja
Nein

The correct import of the certificate you can check within the menu "certificates" of Internet Explorer under menu „trusted **root certification authorities**":

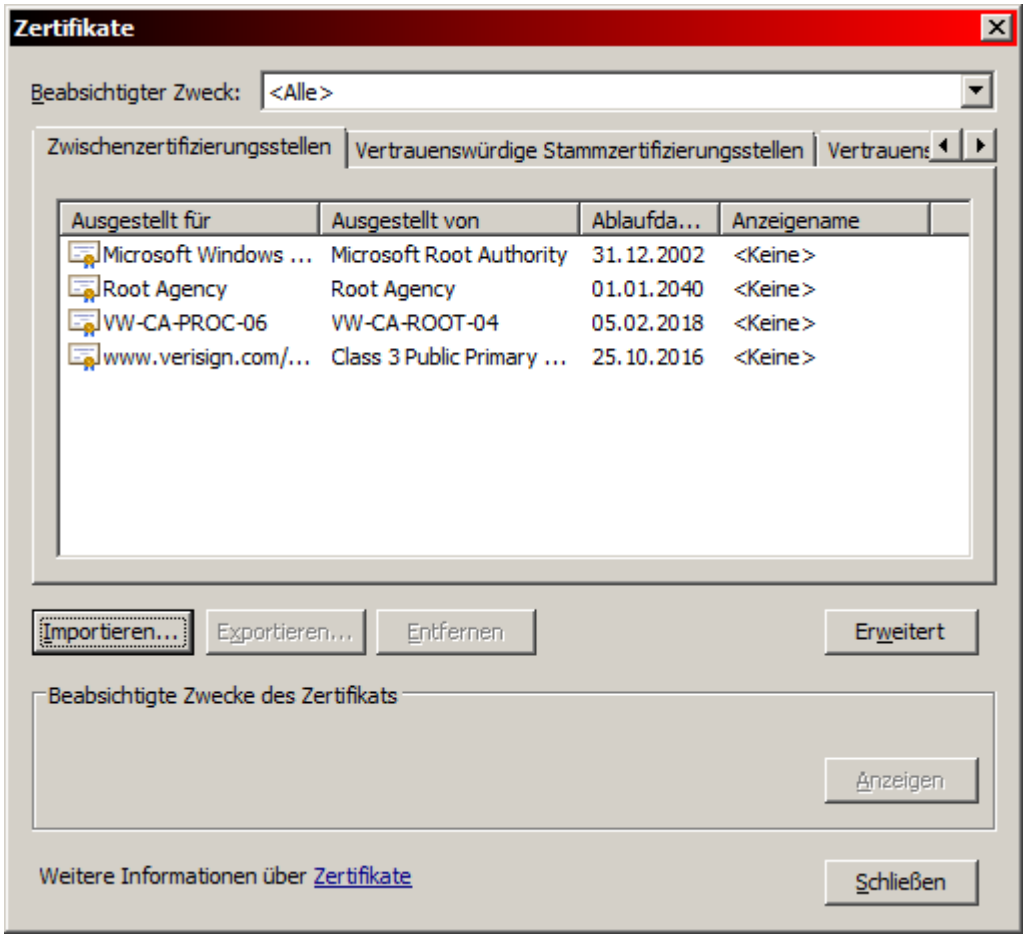

Zertifikate
Beabsichtigter Zweck: <Alle>
Zwischenzertifizierungsstellen
Vertrauenswürdige Stammzertifizierungsstellen
Vertrauens
Ausgestellt für | Ausgestellt von | Ablaufda... | Anzeigename
NO LIABILITY ACC... | NO LIABILITY ACCEP... | 08.01.2004 | VeriSign Time St...
Thawte Premium Se... | Thawte Premium Serv... | 01.01.2021 | thawte
thawte Primary Ro... | thawte Primary Root CA | 17.07.2036 | thawte
Thawte Timestampi... | Thawte Timestamping... | 01.01.2021 | Thawte Timesta...
UTN-USERFirst-Obj... | UTN-USERFirst-Object | 09.07.2019 | USERTrust
VeriSign Class 3 Pu... | VeriSign Class 3 Public... | 17.07.2036 | VeriSign
VeriSign Trust Netw... | VeriSign Trust Network | 19.05.2018 | VeriSign
VeriSign Trust Netw... | VeriSign Trust Network | 02.08.2028 | VeriSign
VW-CA-ROOT-04 | VW-CA-ROOT-04 | 15.03.2018 | <Keine>
Importieren...
Exportieren...
Entfernen
Erweitert
Beabsichtigte Zwecke des Zertifikats
Anzeigen
Weitere Informationen über Zertifikate
Schließen

VW-CA-PROC-06:

Internet Explorer under settings/options → content → certificate → choose „trusted **intermediate certification authorities**" → import → import VW-CA-PROC-06 certificate.

Confirm the warning with „Yes".

This certificate you will find unter menu „certificates -> „trusted **intermediate certification authorities**":



2 CAD data exchange via OFTP2

As a different to OFTP1 with Odette File Transfer Protocol 2 (OFTP2) it is possible, to send and receive data encrypted via Internet between the supplier and Volkswagen/Audi. This protocol is recommended by VDA (association of the German automotive industry) too.
With OFTP2 a SSL/ TLS-encrypted TCP/IP connection will be established.
Each TCP/IP package will be encrypted. Files have only been encrypted if they were saved or routed from a provider. The supplier will get the necessary OFTP2 certificate for TLS encryption from VDA.
For OFTP2 data exchange special OFTP software is necessary that supports this protocol.
For further information please see your software documentation or ask your software supplier directly. The following information will help you to prepare your new OFTP2 receiving station.

2.1 OFTP installation of a company

If a company exchanges OFTP data with Volkswagen/Audi for the first time, an OFTP station entry on the OFTP server systems of VW/Audi needs to be generated. For doing this we need your Odette ID as well as the ODETTE certificate for the encrypted data exchange.
After that, you will get a triple-digit identification code, the passwords for sending and receiving data as well as the ODETTE certificate from Volkswagen. These settings must be configured in your OFTP software. For the preparation of an OFTP station entry an Odette-ID and an ODETTE certificate are absolutely necessary.

2.2 OFTP server at Volkswagen

Normally your software supplier will set up the OFTP server in your communication software. Therefore the following information is required (station RF2):

IP-Address for incoming calls (TLS):
oftpv2cad.volkswagen.de (194.114.32.59) Port 6619 (-you have to call this address)

IP-Address for outgoing calls (TLS):
194.114.40.215 and -.216 (Volkswagen and Audi are calling from these addresses)

ODETTE SSID code (OFTP2 VOLKSWAGEN Gateway SID=RF2):
O0013000001VW……RF2 (first sign is the letter "O"; 6 blanks in front of RF2)

ODETTE SFID code (OFTP2 remote partner SID=RF3 from the VW Group):
O0013000001VW……RF3 (first sign is the letter "O"; 6 blanks in front of RF3)

With help of the certificate restricted list (CRL) of the ODETTE organization you can check the validation of the Volkswagen certificate: http://www.odetteca.com/Repository/ODETTE%20Root/ODETTE%20Root.crl

In case this is not possible, we can provide the certificate for installation within your OFTP2 software alternatively.

Please note: data file encryption is not supported; only TLS1 is used.
The connection set-up will be done without OFTP authentication. The TLS receiver has to be activated.

Passwords are transmitted during the final connection test by one of our supporters.

2.3 Configuration of firewall

The port 6619 will be used for the OFTP2 data exchange. This port must be enabled on the firewall.

2.4 Default settings / ENGDAT parameter

All files are always sent gzip packed and must be unpacked upon receipt!

Volkswagen/Audi only receives and sends files via ENGDAT. While sending via ENGDAT, please pay attention to the following information:

- The ENGDAT transmission address must not be copied to the ENGDAT file name!

- The transmission address must be entered in UNB-0014 segment of the abstract file.

2.5 Handover to operation support / connection test

During the final connection test (appointments are arranged with Service Support Center of operational services), the following items will be tested:

> OFTP communication between the OFTP server of companies and the OFTP servers at Volkswagen/Audi is established via a "LOOPTEST". To this effect, a file with arbitrary content (volume not to exceed 10 kB) is sent to the receiver station RF3 at Volkswagen with the name <LOOPTEST>.
> If successfully received, the file is automatically sent back to the sender. After the receipt of the LOOPTEST, the file data transfer in both directions is guaranteed. You can utilize your newly installed connection for data exchange after a successful "LOOPTEST".

3 CONNECT

The CONNECT Client is a framework for collection, distribution, configuration and launch of the main CONNECT and Teamcenter applications. The CONNECT Client provides the methods and the common user interface of the GRX Kernel which is the basis for other reference installations, as well (e.g. GRC, GRI).

The CONNECT Client is available for the platforms Windows64, SunOS 5.10, RedHat Linux 5 / 6. SunOS- and Linux versions have been designed for server applications respectively for a dedicated user circle.
The CONNECT Client is distributed in the form of an installer package that can be deployed, unzipped and installed on a CAD-workstation. The instance specific configuration, as well as the related client plugins are deployed on a HTTP server (the so called "CONNECT Client configuration server) by CONNECT application management and support team (AMS).

3.1 System requirements

The following system requirements are valid for both the installation and the use of the CONNECT Client.

3.1.1 Hardware

- CAD workstation with the following specification:
  - Processor platforms: x64 (AMD oder Intel) 64-Bit
  - Processor speed: SPECint_rate2006 value of min. 30.0
  - Free disk space : 20 GB (min. für Installer, application, FCC Cache)
  - Graphics card: Compatible with Teamcenter VisMockup
  - The so called "CAD-Workstation" (VW Client Management) should fulfill the system requirements stated.
- Authentication Tokens:
  - RSA SecurID token

    Regarding the token application a group User-ID is necessary for each user.
    A description for the application process of an User-ID and the necessary application form you will find within the ePortal under: https://e2epfn.pfn.vwg.

3.1.2 Software

- Operating Systems:
  - Linux (VW internally, only VisMockup)
  - Solaris (VW internally, system interfaces only)
  - Windows 7 Enterprise 64bit
- CATIA:
  - Group Reference (GRC 4.4.0 and higher)
    for usage of the CONNECT AFT interface and the CATIMAN image
    ...or...

Any CATIA installation including Release 19 ServicePack 9 Hotfix >= 86 (VW OEM standard) for the CATIMAN image (additional customizing necessary

- Microsoft Internet Explorer 6.0, 7.0, 8.0, (9.0 at 8.3.1.1) (for SSO authentication, Windows only)
- Java JRE 1.7.0_01 oder higher (for SSO authentication, Windows only)

3.1.3 Infrastructure and System Environment

- Network Link to VW Network:
  - Protocol: tcp/ip
  - Min. bandwidth 1.5 Mbps per user.
    In order to cope with load peaks a min. bandwidth of 10 Mbps is recommended.
  - i.e. for 1 to 5 users => bandwidth of min. 10 Mbps
  - Additional users => +1.5 Mbps
  - Latency: RTT für meta data < 100ms
  - The performance for data transfer of big files (e.g. JT, CATparts etc.) increases with higher bandwidth and lower latency.
  - Access to CONNECT servers
- User-home must not be located on a network share. Environment variables APPDATA and USERPROFILE must point to a local directory.

More details you will find within the user manual "CONNECT Client" with assignment.

4 Volkswagen DMS

4.1 System requirements

System resources:

We recommend JavaRuntime 1.6.0.26 (Sun Microsystems). The installation will be run by your system administrator.

Necessary user resources:

- VW-UserID
- RSA SecurID Token

Requirements for workplace

- minimum 2GHz processor
- minimum 4 GB main storage
- adequate hard drive space

4.2 Settings

Webserver:
https://vwdmsweb.pfn.vwg/vwdms (193.23.101.113)